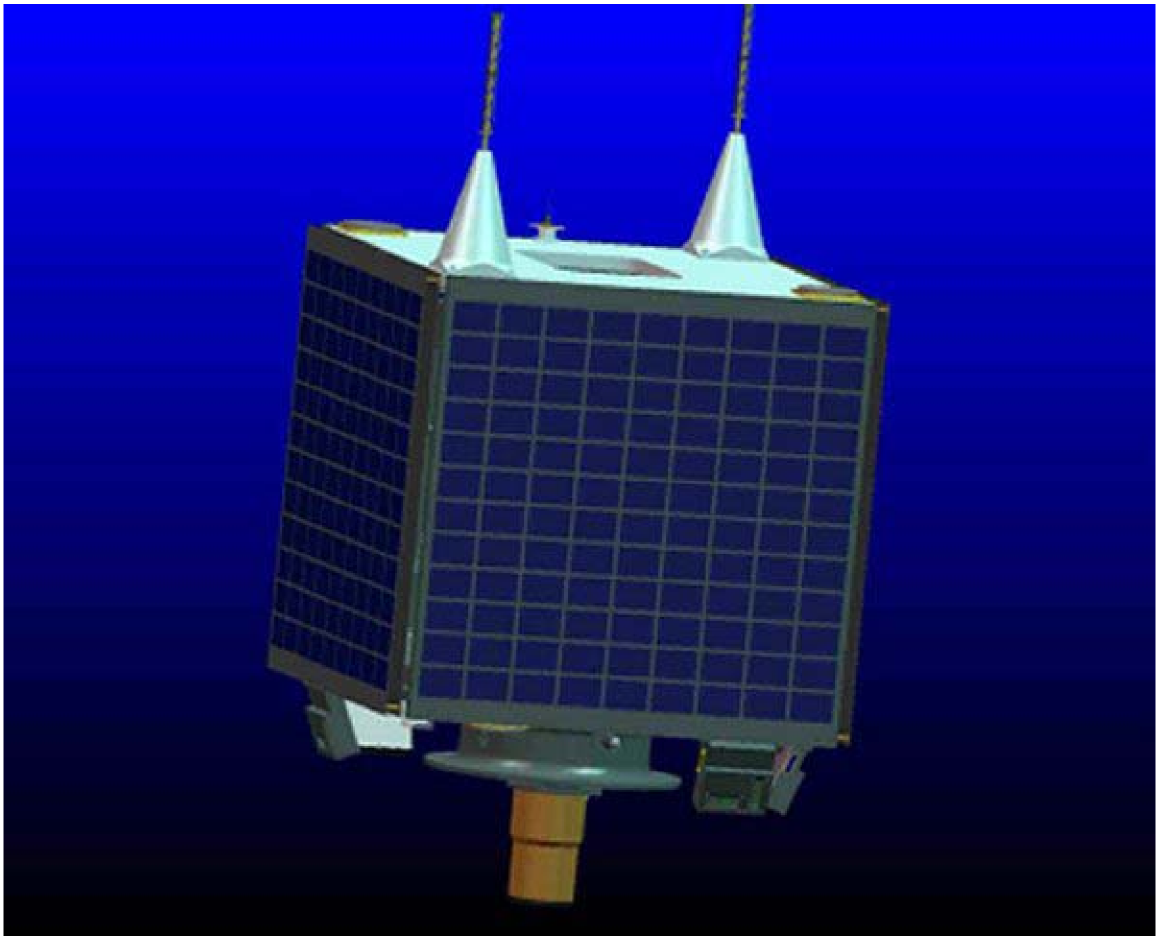


CLEO

Cisco Router in Low Earth Orbit

Phil Ardire, Terry Bell, Brett Conner PhD, Larry Dikeman, Donald Van Drei, Steve Groves, William Ivancic, Eric Miller, Phillip Paulsen, Dan Shell, Dave Stewart, and Lloyd Wood

January 29, 2004

Abstract

This paper discusses a joint demonstration, currently underway, with the Air Force and Army Space Battle Labs, NASA GRC, NASA GSFC, Cisco, Western DataCom, Surrey Satellite Technologies Limited, and General Dynamics. This demonstration will highlight the flight of COTS network device (a miniature router) aboard an experimental micro-satellite that is controlled remotely using an Internet Protocol-based satellite command and control application that provides secure, virtual mission operations. The new architecture, showcased through this demonstration, is intended to meet the security, survivability, and rapid re-configuration requirements typically found in a complex research or battlefield environment. The results of this demonstration are intended to be used by those designing and fielding future integrated land, sea, air, and space core network elements.

The Transformational Communications Office is currently defining the next-generation, joint NASA and DOD communications architecture. It will utilize Internet Protocols to standardize Tracking Telemetry and Control (TT&C) elements to ensure seamless interoperability between land, sea, air, and satellite-based systems. This task is daunting and more complex than any that has been attempted to date. In order to maximize the likelihood of success, a number of different entities (both public and private) are currently involved in research aimed at defining key elements of the architecture.

NASA's Glenn Research Center (GRC) and its consortium partners have been heavily involved in the development of Internet technologies for space applications since the mid-1990's, utilizing GRC's Advanced Communication Technology Satellite (ACTS) as a networked systems test bed. Today, GRC's cooperative research, funded by NASA's Earth Science Technology Office, is concentrating on the development of secure, mobile network hardware, software, protocols, and operations applications for use in a wide variety of platforms, including satellites, aircraft, unmanned vehicles, ships, and launch vehicles.

GRC's current development activities all utilize, to the greatest extent possible, commercial-off-the-shelf (COTS) network equipment that has been designed to open standards, helping to reduce costs and ensure compatibility with future commercial systems. To date, this secure, mobile network research has been conducted using government satellite systems (ACTS and the Tracking and Data Relay Satellite System [TDRSS]), commercial satellites (Iridium and Globalstar), as well as mobile terrestrial communications platforms such as military vehicles and ships. GRC has worked closely with several vendors to aid in the development of commercial products which may ultimately be used in space. Examples include Cisco (a miniaturized router), Western DataCom (a miniaturized encryption device), and General Dynamics (a virtual, Internet Protocol-based Satellite Command and Control System).

Table of Contents

Drawing List

Background

One of the three elements in the NASA Vision is "to improve life here". The lead NASA Enterprise for this vision element is Earth Science (ESE). Using the vantage point of space, NASA gains an understanding of our home planet that could otherwise never be achieved[1.] The ESE provides accurate, objective scientific data and analysis to advance the understanding of Earth system processes. They pursue answers to the fundamental question,

> “How is the Earth changing and what are the consequences for life on Earth?”[2]

New capabilities in scientific observations and modeling are enabling the integrated evaluation of ecosystems in the air, on land, and at sea. These new capabilities, when coupled with climate change forecasts are expected to allow future researchers to more accurately predict future impacts of climate variability or policy changes on life on Earth. To achieve this goal, the measurements of all the major Earth Science observation components (climate, ocean, weather, biosphere, water cycle, atmospheric composition, radiation budget, and Earth crustal movement) will need to be integrated into a comprehensive Earth System Model that can link causes, effects and relationships into one complete understanding of the Earth system.[3]

Today, the Nation has a system of satellites with the ability to characterize the current state of the Earth system. In collaboration with our research partners, the Earth Science community intends to further the understanding of the Earth system through the integration of satellite, suborbital and surface measurements in conjunction with models that simulate links and feedback between Earth system processes. In the years ahead, Earth-orbiting satellites are expected to evolve into constellations of smart satellites that can be reconfigured based on the changing needs of science and technology. The data from these satellites will be integrated with an intelligent observation network composed of sensors deployed in vantage points from the subsurface to deep space. This “Sensor Web” will provide on-demand data and analysis to a wide range of end users in a timely and cost-effective manner. These data and information products will be used in Earth system models by NASA, NOAA, NSF, and DOE to assess and predict Earth system change.[4]

The long-term vision of the Sensor Web observing architecture employs large numbers of frequency-agile sensors operating from multiple vantage points to simultaneously collect suites of observations from multiple regions. The capability to tailor the spatial, spectral and temporal resolution of the measurements will be accomplished by having a cooperating fleet of spacecraft operating intelligently. Such an architecture requires advanced on-board data processing systems capable of orchestrating real-time collaborative operations. For such an observing system, information technology investments are needed to develop the capability to observe autonomously in a changing environment, and to rapidly convert vast amounts of sensor data into operational knowledge and information products.[5]

The Earth Science Technology Office (ESTO) invests in technologies on behalf of the Earth Science Enterprise. The goal of ESTO is to reduce the risk, cost, size and development time of ESE systems; increasing the accessibility and utility of Earth science data; and enabling new Earth observation measurements and information products. These Earth Science technology investment projects facilitate the adaptation of instrument and information systems technology that will be needed to support future Earth Science measurements.[6]

In 2000, using ESTO funding (combined with funding from CICT and SOMO,) NASA GRC initiated a series of satellite accommodation studies with four satellite vendors (TRW, Spectrum Astro, Orbital Sciences, and Surrey Satellite Technologies [SSTL]) to address the potential cost and impact of using Internet Protocols (IP) on board satellites, with the goal of making each future satellite just "another node on the Internet". Somewhat surprisingly, three of the four vendors indicated that the use of IP onboard spacecraft was not only feasible, but that it would be to the Government's advantage to make the change.

Satellites are typically custom built and require a number of proprietary interfaces. Each satellite consists of a primary bus, surrounded by one or more instruments, all of which are provided by different vendors. Because each satellite bus and each instrument is unique, interface control documents (ICDs) are required to document and manage each interface. Although exhaustive, these documents are not always 100% successful at uncovering each interface issue. Integrated testing, where interface issues are normally uncovered, typically occurs very late in the satellite build process (normally after the satellite bus and each individual instrument has been through its own separate qualification program). Thus, integrated testing usually occurs when it is too late to make wholesale design changes without affecting schedule. Problems uncovered late in a program can be extremely expensive to correct and usually result in significant launch delays.

Considering a typical satellite program, the cost of a satellite can be summed by including such things as:

1. Materials (steel, ceramics, aluminum, etc…)
2. Avionics
3. Software
4. Nitrogen, hypergols, and other consumables
5. Tooling
6. Personnel (the engineers and technicians required to design, build, integrate, test, and operate the spacecraft)

Of these six items, the number of personnel and the length of their project tenure is often the only variable that can be meaningfully impacted when attempting to reduce overall mission life cycle costs. Anything that can meaningfully reduce the length of time that the "standing army" is required can have a tremendous impact on the total satellite life cycle cost. According to the study vendors, the use of common IP interfaces has the potential to dramatically reduce the total time required to design, build, test, and validate spacecraft. Additionally, with the use of common interfaces, integrated satellite testing can begin far earlier, by using a terrestrial Internet connection to bridge the communications gap between the satellite bus and instruments, prior to full scale qualification. This early testing, performed while the satellite bus and the individual instruments are still in their respective factories, is expected to uncover integration issues early, while it is still relatively inexpensive to make the necessary design changes and avoid launch delays.

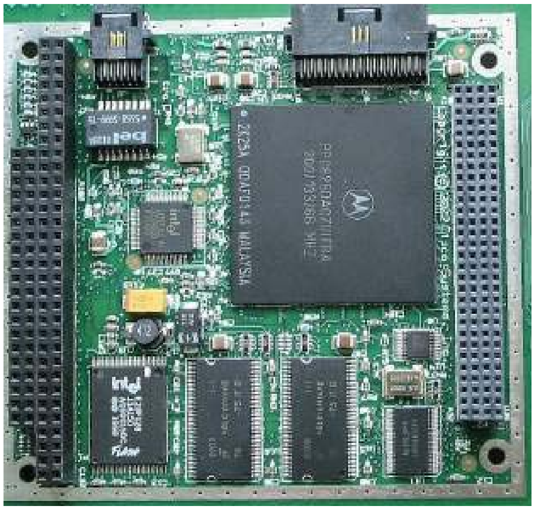
Use of common IP interfaces also extends beyond the satellite development process. Typically, satellites arrive at the launch site payload processing facility (PPF) with unique terrestrial interface requirements to facilitate ground-based testing. Being able to accommodate these unique interfaces often results in the expenditure of significant amounts of time and capital. Similarly, when a satellite is mated to an expendable launch vehicle (ELV,) it usually requires a mission unique interface with the ELV data system to accommodate satellite health status data during flight. The integration of the two proprietary systems usually requires further accommodation and capital expenditures. Replacement of proprietary interfaces with common IP interfaces could result in a cost savings in terms of funding and time in both the PFF and on board the ELV. To this end, the National Reconnaissance Office (NRO) has already designed and built a standard commercial-off-the-shelf (COTS) IP interface rack that will be provided generically to all future satellite vendors as Government Furnished Equipment (GFE). These GFE racks will be used as "the" interface in the factory during satellite design, build, and test, in the PPF during spacecraft integration, test, and fueling, and in the launch tower complex as a part of the final testing aboard the ELV.

Finally, the use of COTS IP interfaces can also impact the cost of ground station design and operations. Typical ground station procurements are let fairly late in the satellite procurement process (often after the satellite design work has largely been completed) and may involve multiple, unrelated vendors. Because of the proprietary nature of today's satellites, this often results in major integration issues late in the program, further driving up costs. The use of COTS IP interfaces aboard satellites is expected to help eliminate many of the design issues associated with the proprietary data interfaces. Additionally, since commercial ground station providers are already using COTS IP in their terrestrial networks, the use of similar interfaces on satellites is attractive, since the new interfaces are expected to eliminate many of the normal integration issues. With the new IP-compliant systems, data will be shipped directly from the satellite, to the ground, and on to remote user locations without the need for protocol conversion (which is typical with today's systems) eliminating the need for mission unique software to perform the conversion on the ground.

Because of the promise of this technology, both NASA and the DOD are currently working together on a new, integrated communications architecture. Called the, "Transformational Communications Architecture" or "TCA", it is expected to offer seamless interoperability between terrestrial (land, sea, and air) and satellite-based systems by utilizing COTS IP across all domains. NASA GRC and its consortium partners have been involved in the development of requirements for the TCA. During the development of the TCA requirements, GRC performed an informal gap analysis to determine what technologies need to be developed in support of the new architecture. The key technologies include space tolerant network device designs, "virtual" satellite operations concepts, and integrated information assurance concepts. Considering each:

Space Tolerant Network Devices

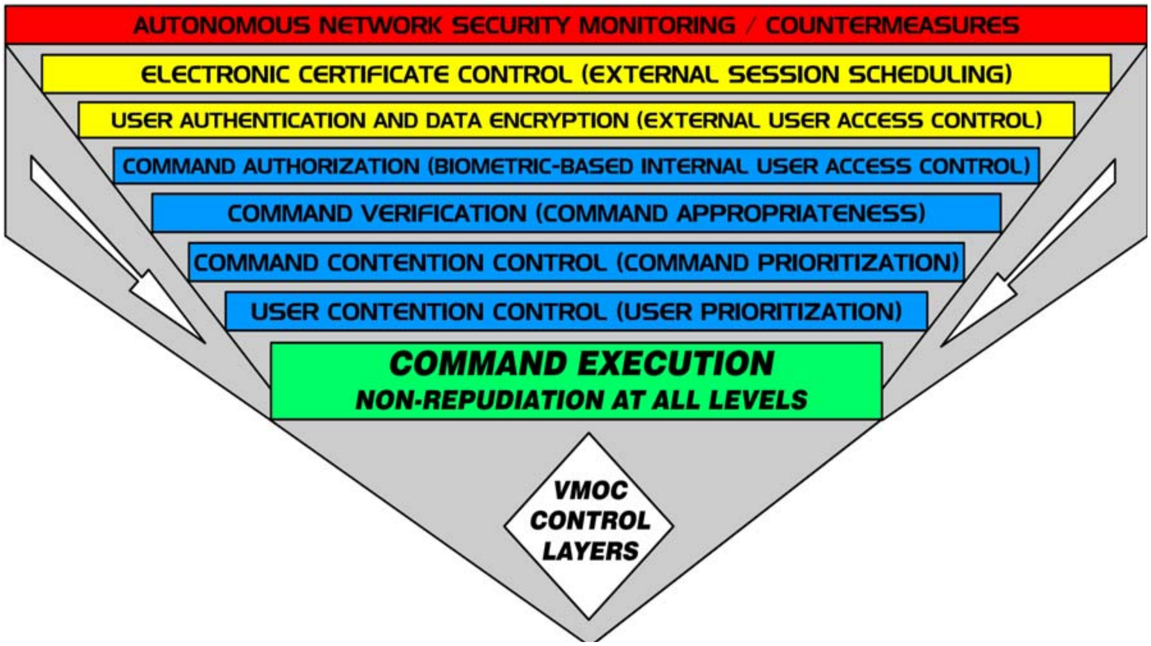
Terrestrial network devices tend to be large, heavy, and power inefficient. They are not radiation tolerant. The TCA is expected to accommodate a wide variety of user classes with data rates ranging from kilo bits per second (kbps) to multiple giga bits per second (Gbps). To maximize system efficiency and reduce project cost, this will require the development of multiple network device classes. For missions requiring IP-compliant devices that operate at 100 mega bits per second (Mbps) or less, Cisco has developed a fully featured, miniature router (Figure A). It is relatively small (2 cards, PC-104 form factor, roughly 4" on a side), lightweight, and consumes 10 Watts of power while operating. The mini-router offers the full functionality of the Cisco Internetwork Operating System (IOS) and it is built to conform to the latest open standards (as maintained by the IETF), guaranteeing seamless interoperability with other terrestrial network devices. Finally, it is compliant with the latest open standards for mobility (called "Mobile Router"). This innovation, developed by the IETF and evaluated at GRC, allows entire networks to move from one operating theater to another without the need for manual reconfiguration of routers or hosts.



Cisco Miniature Router
Figure A

Virtual Mission Operations

The use of IP onboard spacecraft allows the use of completely new operations models. Beginning in 1999, NASA GRC began looking at the operational implications of using IP in space. Called “Virtual Mission Operations” (VMO), it is the first attempt in creating a secure application for the remote command and control of space-based assets. Working collaboratively with General Dynamics (formerly Veridian Information Solutions, a leading network security vendor for the intelligence community) and operations specialists from the Johnson Space Center’s (JSC’s) Mission Control Center (MCC), requirements for generic mission operations were developed. These requirements were then captured in the model shown in Figure B:

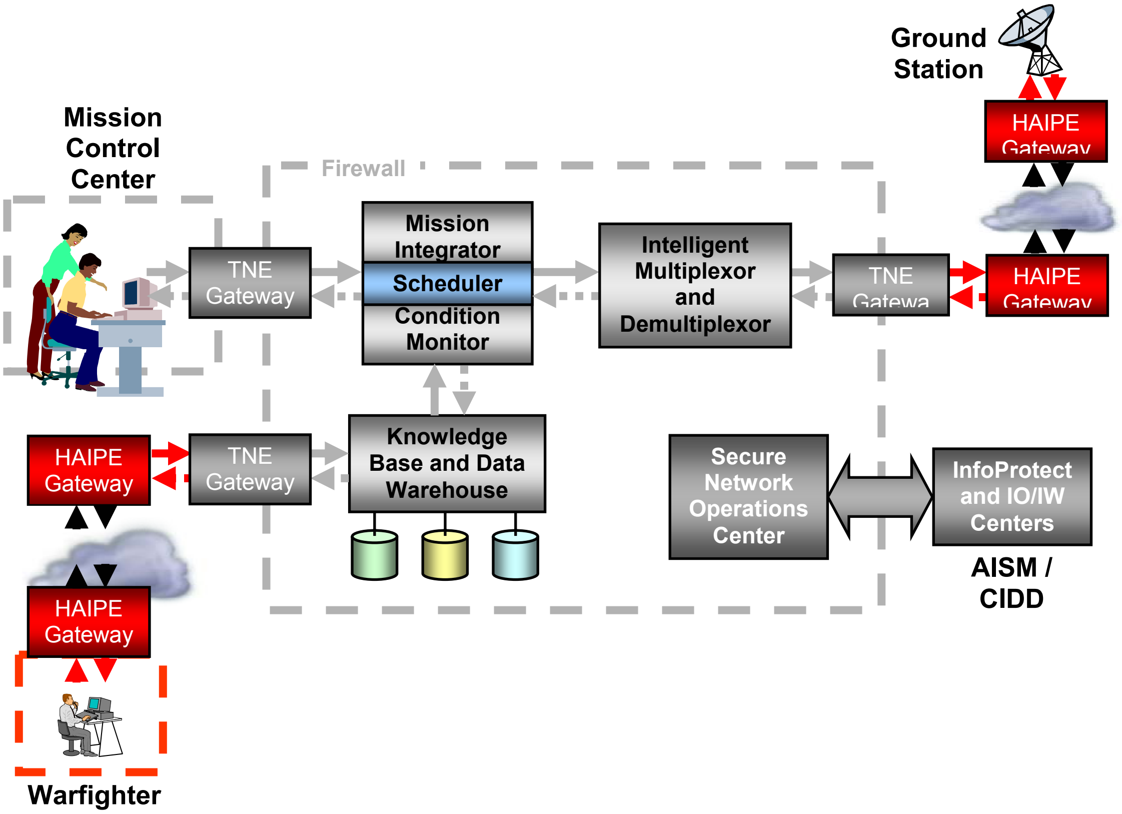

AUTONOMOUS NETWORK SECURITY MONITORING / COUNTERMEASURES
ELECTRONIC CERTIFICATE CONTROL (EXTERNAL SESSION SCHEDULING)
USER AUTHENTICATION AND DATA ENCRYPTION (EXTERNAL USER ACCESS CONTROL)
COMMAND AUTHORIZATION (BIOMETRIC-BASED INTERNAL USER ACCESS CONTROL)
COMMAND VERIFICATION (COMMAND APPROPRIATENESS)
COMMAND CONTENTION CONTROL (COMMAND PRIORITIZATION)
USER CONTENTION CONTROL (USER PRIORITIZATION)
COMMAND EXECUTION
NON-REPUDIATION AT ALL LEVELS
VMOC CONTROL LAYERS

GD's Virtual Mission Operations Model
Figure B

This model was also captured in software by GD and successfully demonstrated at JSC's "Inspection 2000" open house event. For purposes of the demonstration, NASA's Goddard Space Flight Center (GSFC) provided a networked connection over a geostationary TDRSS satellite using a device called TILT. NASA GRC provided land line network connections and an emulated International Space Station experiment. GD provided the VMO software suite. Based on the positive reaction from the satellite community, GRC placed GD on contract to further refine the VMO model and capture the knowledge gained (GD also provided a matching sum of internal research and development funding on the project).

GD's initiative, (named Nautilus Horizon), provides a framework for mission partners to define, test, validate, and field an IP-based command and control system capable of supporting secure, distributed mission operations of any IP-based platform or sensor. Central to their concept is the Virtual Mission Operations Center or VMOC which performs a number of functions:

1) Enables system operators and data users to be remote.
2) Verifies individual users and their authorizations.
3) Establishes a secure user session with the platform.
4) Performs user / command prioritization and contention control.
5) Applies mission rules and performs command appropriateness tests.
6) Relays data directly to the remote user without human intervention.
7) Provides a knowledge data base and is designed to allow interaction with other, similar systems.
8) Provides an encrypted gateway for "unsophisticated" user access (remote users of science data).



GD's Virtual Mission Operations Center (VMOC)
Figure C

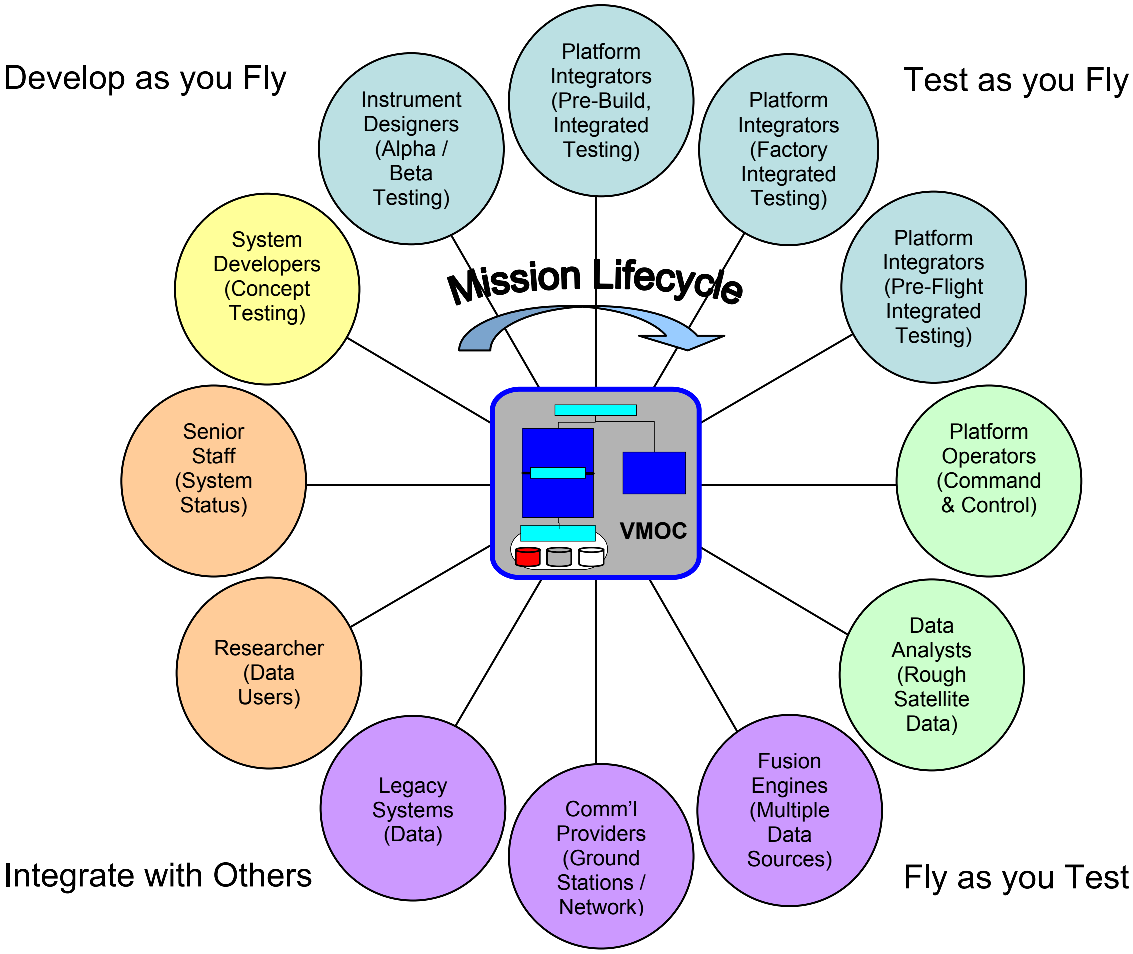
As a "virtual" entity, the VMOC (Figure C) can exist at any location that has enough network bandwidth to support operations. It can also be replicated and mirrored at multiple locations to reduce the likelihood of a single catastrophic event precluding continued operations, without the need for a large operations staff at each remote location. With the knowledge database installed, it will be possible to use peer-to-peer networking tools to improve data distribution efficiency and reduce unnecessary satellite operations to regenerate data. The VMOC has also been designed to easily accommodate data mining tools to track and predict individual user data requirements, providing feedback to system operators to further refine and optimize system operations.

As currently envisioned, the VMOC that will eventually be fielded as an operational element under the new Transformational Communications Architecture will not be limited to the direct command and control of platforms. Instead, the VMOC will provide support in three primary areas:

1. **Policy**
   The VMOC platform will provide an interface for command organizations to establish and promulgate system policy across a body of users.

2. **User**
   The VMOC platform will provide a standards-driven common user interface for controlled access to platforms, sensors, and the information generated by each.
3. **Mission**
   The VMOC platform will enable policy-based tasking and prioritization, as well as a machine-to-machine interface, minimizing or eliminating the requirements for a man-in-the loop.

Recognizing the wide variability of user requirements across the product life cycle of a typical mission, the VMOC has been designed to incorporate tool reuse and be as flexible as possible. Referring to Figure D, the same basic tools are expected to be used during system conceptual development, test, integration, validation, and operations. These tools will also offer “hooks” to accommodate integrated operations with other platforms and data sources, plus, the system will provide statusing to senior managers and other system owners. Finally, the VMOC will incorporate a data user interface to allow controlled system entrance and interoperation at the data level, without requiring individual users to be knowledgeable concerning overall platform design or operations. This “unsophisticated” user will be able to access stored data and indirectly task operational elements through data requests.


Develop as you Fly
Test as you Fly
Integrate with Others
Fly as you Test
Mission Lifecycle
VMOC
Instrument Designers (Alpha / Beta Testing)
Platform Integrators (Pre-Build, Integrated Testing)
Platform Integrators (Factory Integrated Testing)
System Developers (Concept Testing)
Platform Integrators (Pre-Flight Integrated Testing)
Senior Staff (System Status)
Platform Operators (Command & Control)
Researcher (Data Users)
Data Analysts (Rough Satellite Data)
Legacy Systems (Data)
Comm'l Providers (Ground Stations / Network)
Fusion Engines (Multiple Data Sources)

VMOC Support Across the Product Life Cycle
Figure D

Integrated Information Assurance

As new IP compliant systems begin to emerge, information operations that protect and defend the systems themselves and the information that they carry will be critical to the success of the mission. To effectively resist attacks on its information and information systems, an organization must characterize its adversaries, their potential motivations, and their attack capabilities. Potential adversaries might include nation states, terrorists, criminal elements, hackers, or corporate competitors. Their motivations might include intelligence gathering, theft of intellectual property, causing embarrassment, or just anticipated pride in having exploited a notable target. The methods of attack might include passive monitoring of communications, active network attacks, close-in attacks, exploitation of insiders, and attacks through the industry providers of the organization's information technology (IT) resources.[7]

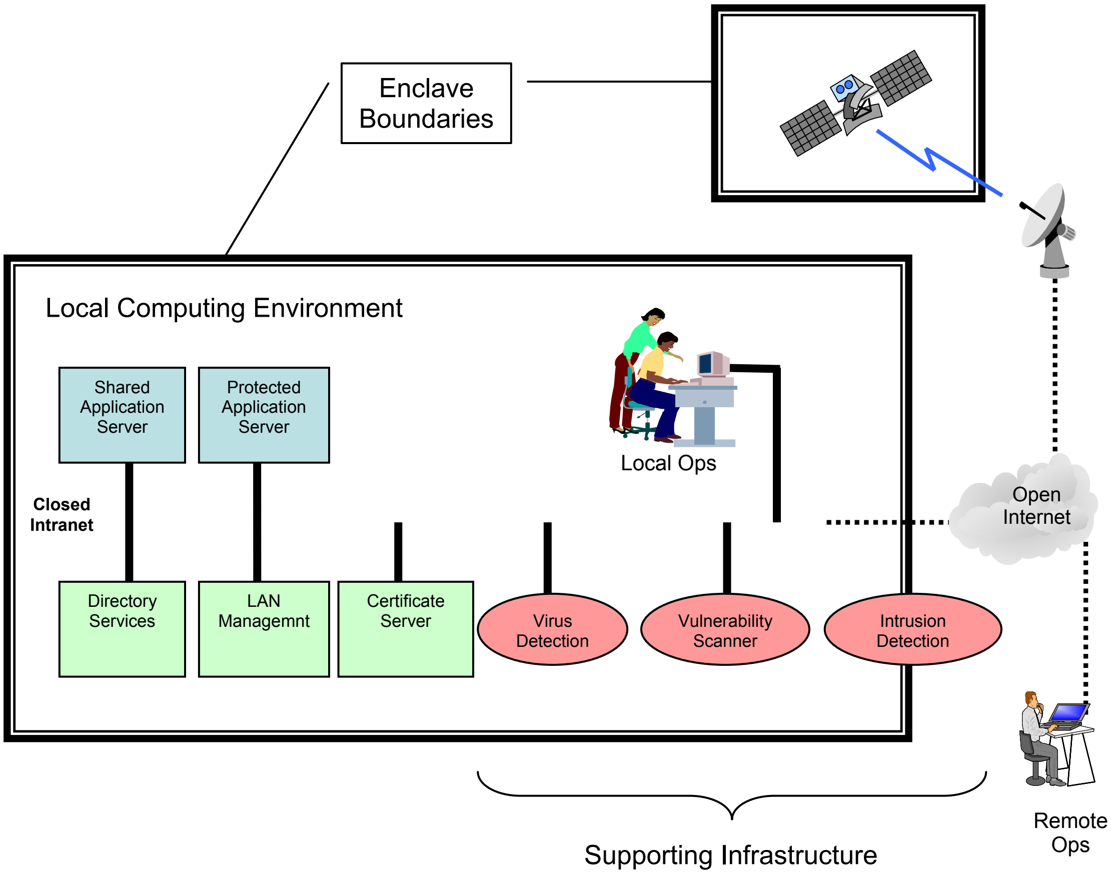
NSA defines four distinct areas that require information protection (Figure E):

1. Local computing environments (local Intranets containing servers, clients, and the applications installed on them).

2. Enclave boundaries (a collection of local computing devices interconnected via Local Area Networks [LAN], governed by a single security policy, regardless of physical location).

3. Networks and infrastructures (A collection of public and private network resources providing connectivity between enclaves. The transport networks contain the information transmission components [e.g., satellites, microwave, other Radio Frequency {RF} spectrum, and fiber] to move information between the network nodes [e.g., routers and switches]).

4. Supporting infrastructures (a collection of devices for securely managing the system and providing security-enabled services for networks, end-user workstations, servers for Web, applications, and files, and single-use infrastructure machines [e.g., higher-level Domain Name Server {DNS} services, higher-level directory servers]. The support infrastructure also includes the key management infrastructure [KMI, which includes Public Key Infrastructures {PKI}], and detect and respond infrastructures).[8]



Areas of Information Assurance Interest
Figure E

For purposes of this research project, a fairly complex arrangement of local computing environments, enclaves, networks, infrastructures, and supporting infrastructures will be deployed and evaluated for efficacy and usability. In each area, issues related to system / data availability, integrity, authentication, confidentiality, auditing, countermeasures, and non-repudiation will be addressed.

Today's terrestrial data networks routinely move data using Internet Protocols. Most, if not all, systems with satellite command and control interfaces use purely closed systems (physically segregated from other, non-command and control users). Future systems will very likely accommodate user access (and system command and control) via open systems. This will extend the reach and usability of the future systems (and reduce overall system costs by taking advantage of shared network infrastructure) at the potential cost of adding additional mission risk. We believe that these risks are manageable and that the benefits associated with such a change will far outweigh the cost. For purposes of this project, a demonstration of secure command and control of a space-based asset over both public and private network resources will be accomplished. The demonstration will include such thing as automated methods for user authentication (biometrics, passwords, common access cards, etc…), user access control, data integrity checks, and system auditing. Autonomous network intrusion detection and countermeasures will be conducted using the Automated Security Incident Measurement (ASIM) intrusion detection system and the Common Intrusion Detection Director (CIDD). Both AISM and CIDD were developed by GD for the Air Force Information Warfare Center (AFIWC) and they are used routinely by most DOD bases to mitigate the network risks associated with hackers (external to the monitored connections) and saboteurs (internal to the monitored connections).

As a part of our research program, NASA GRC has also been exploring new encryption technologies to connect secure enclaves and securely transition open infrastructure. In 2002 GRC and its consortium partners performed a demonstration aboard the USCG Neah Bay (a US Coast Guard ice breaker stationed in Cleveland, Ohio) that included secure data exchange between the ship (at sea) and a closed network (.mil) over a commercial satellite (Globalstar) with a data touchdown point in a foreign country (Canada), over the open Internet. This was accomplished using an end-to-end network architecture featuring an encryption device which utilized NSA's new High Assurance Internet Protocol Encryption (HAIPE) data formatting, triple DES, and 168 bit keys. Future systems which require secure communications are expected to utilize HAIPE, which comes in three "strengths": top secret (Type 1), secret, and coalition to ensure data integrity and confidentiality. Future IP compliant command and control elements (and DOD payload data) will likely require Type 1 HAIPE encryption. NASA payload data (often generated by instruments provided by foreign partners) will probably be flown with coalition strength HAIPE encryption. By utilizing HAIPE encryption, firewalls can effectively be extended through the open Internet to a remote user location. In addition, virtual private networks (VPNs) can also be used to secure communications through the open Internet. Due to time and satellite power constraints, HAIPE encryption was not included in the mission package being flown as a part of this project. For purposes of this project, a demonstration of terrestrial fixed and mobile encryption technologies (linking secure enclaves) will be accomplished.

The Demonstration

Although the equipment and virtual mission operations techniques have been thoroughly demonstrated in the terrestrial environment, the risk adverse nature of the space community typically requires flight demonstration prior to full scale implementation. To date, there have been a number of early demonstrations of IP in Space. Since the 1980's research has been conducted into the use of IP through space (in a bent pipe fashion over geostationary communications satellites). Since the mid-1990's, four research satellites have successfully flown IP elements:

- STRV-1B (UK Defense Research Agency and JPL)
  - Use of SCPS-TP (1 Kbps space to ground, 125 bps from ground to space)
  - Use of FTP (space to ground)
  - Use of security protocol (space to ground)
  - Use of SNACK and header compression techniques

- UOSAT-12 (SSTL and GSFC)
  - FreeBSD 4.4 IP stack
  - Use of clock synchronization (NTP) client and FTP server
  - End-to-end connectivity (ping) tests
  - Blind commanding
  - Web server (HTTP) tests

- CANDOS (ITT and GSFC)
  - Mobile IP (MIP) from control center to current uplink antenna
  - Multicast Dissemination Protocol (MDP) UDP-based reliable file transfer
  - Network Time Protocol (NTP) clock synchronization
  - UDP telemetry and commanding
  - Secure Shell (SSH) encrypted remote login
  - Secure Copy (SCP) encrypted file transfer

- CHIPSat (Spacedev, University of California [Berkley], and GSFC)
  - End-to-end TCP/IP-based connectivity
  - Windows NT-based mission control software

Although each has incrementally shown the utility of specific Internet Protocols in space, none has demonstrated the viability of using a network device as a primary component aboard a satellite (nor have they demonstrated end-to-end, secure, virtual mission operations techniques). To this end, GRC and its consortium partners are conducting the first end-to-end demonstration of a COTS network device (a router) coupled with a virtual mission operations application in a space flight experiment. The collaborators for this demonstration include:

- NASA GRC
  - Overall mission coordination, research facilities, and space expertise
  - Teamed with Cisco and Western DataCom via a Space Act Agreement
  - On contract with General Dynamics to refine VMOC concept
- Cisco Systems Incorporated
  - Network gear, architecture development, funding and management of SSTL satellite integration, testing, and operations
- Surrey Satellite Technologies Limited (SSTL)

    - Satellite platform development, testing, and operations
- General Dynamics
    - Architecture development, VMOC development, test, and operations
- 14 Air Force (14 AF)
    - Primary DOD Sponsor: Maj. Gen. Hamel
- Office of the Secretary of Defense (OSD)
    - Sponsor of VMOC demonstration
- 50 Space Wing (50 SW)
    - Satellite operations experts
- Air Force Space Battlelab (AF SB)
    - Management of VMOC demonstration
- Space and Missile Center (SMC) / CERES
    - Housing, maintenance, and operations of the primary VMOC
- Army Space and Missile Defense Battle Lab (SMDBL)
    - Management of VMOC demonstration
- NASA Goddard Space Flight Center
    - Secondary ground station support
- Western DataCom
    - Encryption equipment for ground-based 802.11b links
- University of Cincinnati
    - Hyperspectral imagery researcher
- National Security Agency (NSA)
    - CONUS network penetration testing (currently being negotiated)
- Universal Space Networks (USN)
    - Tertiary ground station support (currently being negotiated)

<u>Key Experiment Issues</u>

For the flight experiment to be a complete success a number of key issues must be addressed:

1. Durability
    a. Can a COTS network device survive space flight environments?
2. Interoperability
    a. Can the flight device interoperate fully with existing terrestrial systems built to the latest open, purely commercial standards (i.e those maintained by the IETF)?
3. Transparency
    a. Once configured, is the new mobile network device truly “set and forget”?
4. Mobility
    a. Can the mobile device maintain network contact over a wide variety of domains without requiring manual reconfiguration?
5. Use of Shared Infrastructure

    a. Can the mobile device take advantage of low cost (open) network infrastructure without imposing any undue risk?

6. Security
    a. Can the commands and data to and from the mobile device securely cross multiple domains (i.e. closed, open, government, military, etc…)?
7. Survivability
    a. Can the system be sustained, even if a primary data path fails?

<u>Demonstration Goals</u>

The demonstration hopes to accomplish three primary goals:

1. Fly and compile operations data on the first commercially available network device (a miniature Cisco router) in space.
    a. To be successful, the COTS device will require modification (replacement of terrestrial connectors and liquid filled components) prior to qualification for flight.
    b. Once on orbit, quantified performance of the orbital device will be measured under actual space conditions (vacuum, radiation, etc...)
        1) Power consumption, voltage transients, thermal transients
        2) Performance characterization with sub-optimal links
    c. Network operations will also be demonstrated and quantified on orbit:
        1) Real time TCP/IP session / TELNET / PING / LOG / CONFIG
        2) FTP
        3) SNMP
        4) HTTP
        5) Mobile IP
        6) Mobile Router
        7) UDP
        8) SSH
        9) TFTP
        10) Cisco TCP acceleration (performance enhancing proxy)
    d. Following a thorough evaluation of the device, tests involving the detection of and recovery from unexpected device operations will be conducted (reboot on orbit).
    e. Finally, assuming that a new router image file can be successfully uploaded to the spacecraft, tests will be conducted to verify that the device configuration can be updated or revised on orbit.

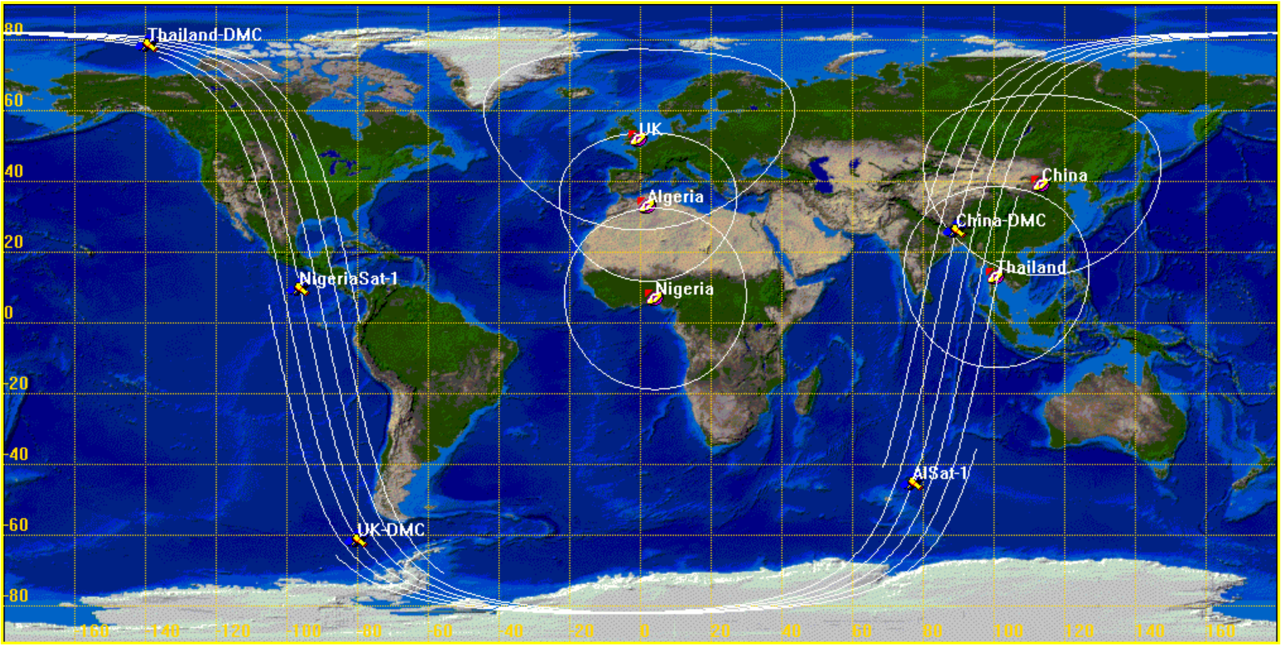
2. Conduct the first secure, survivable, “virtual” mission operations of an element in space.
    a. Autonomous satellite operations from a remote location.
    b. Secure field data dissemination.

c. Secure operations over the open Internet.
d. Validation of multiple users (and contention control).
e. Scheduling access time to spacecraft.
f. Storing and retrieving data from a knowledge database.
g. Predictive routing to appropriate ground station.
    1) SSTL ground station (primary).
    2) GSFC ground station (secondary).
    3) United Space Networks commercial ground station (tertiary – currently being negotiated).
h. Pilot / co-pilot switch over with secondary VMOC.
i. Legacy system support.
    1) Controlled access to satellite data from legacy database.
    2) Secure command and control of the SSTL satellite asset using the VMOC to access and command SSTL's legancy ground system.

3. Conduct the first secure, mobile retrieval of data from a sophisticated system by a mobile researcher.
    a. Tests will demonstrate retrieval of existing data from the VMOC database as well as indirect satellite asset command and control (to obtain data that does not currently exist in the VMOC database).
        1) System / data availability, integrity, user authentication, confidentiality, auditing, countermeasures, and non-repudiation will also be verified during the performance of this demonstration.
        2) Secure mobile network connections (HAIPE / 802.11b).
        3) Unsophisticated user data retrieval interface.
        4) Data mining techniques.
    b. System integrity checks (penetration testing) will also be performed on CONUS-based system elements to validate system integrity.
        1) Unauthorized user detection and mitigation.

Satellite Platform

In order to secure a low cost, high performance space platform, one mission partner, Cisco, turned to Surrey Satellite Technologies Limited (SSTL). SSTL, a British manufacturer of experimental satellites, agreed to host Cisco's device as an experiment aboard one of their current missions. All expenses related to the miniature router experiment, satellite modifications, testing, and operations are being borne by Cisco. The satellite, referred to as DMC-UK (Disaster Monitoring Constellation), is being fielded by the United Kingdom. Each satellite has a different owner (UK, China, Algeria, Thailand, and Nigeria), but acts as one of a constellation of five. At present all five satellites are managed through a ground station at Surrey's parent location, but, eventually, each will possess its own independent ground station in its respective country. To date, four of the five satellites (including DMC-UK) have been successfully flown aboard Russian KOSMOS expendable launch vehicles from Baikanur.



Ground Trace, DMC Constellation
Figure F

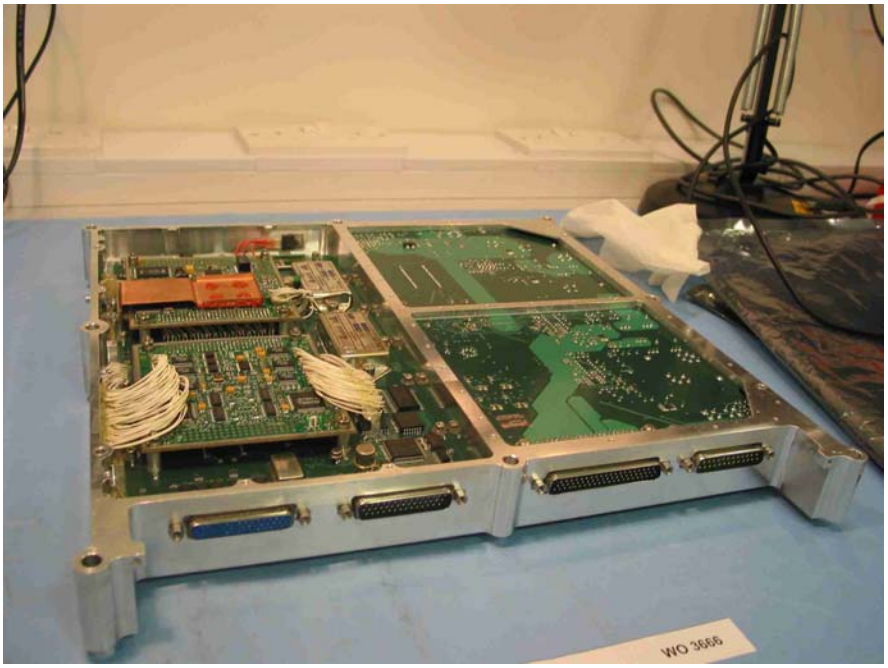
Each satellite has the same physical characteristics:

- 686km, 98 degree inclination, sun sync
- 100kg satellite
- Five year target design life
- Multi-spectral imager (similar to LandSat 2, 3, & 4 Thematic Mapper Bands)
    - 0.52 - 0.62 (Green)
    - 0.63 - 0.69 (Red)
    - 0.76 - 0.9 (NIR)
  - 32m ground resolution
  - 600km push broom swath width
- 8Mbps S-band downlink
  - 3.5m ground station

For purposes of this mission, the DMC-UK satellite carriers an extra experiment tray which houses the Cisco Mobile Access Router (CISCO 3251). It consists of:

- Two 4” x 4” PC-104 compliant cards
  - One router card and one I/O card

- Dual 100BaseT Fast Ethernet ports on main router card (one exclusively for the PCI backplane)
    - PCI backplane connects to a four port serial card
- Maximum of 100 Mbps integrated, duplex throughput (limited by the mission to 8 Mbps downlink, 9.6 kbps uplink).
- Generic IPSEC encryption
- Operates at 5 VDC, 10W



Cisco Router Mounted in a SSTL Experiment Tray
Figure G

For purposes of the demonstration, the CISCO 3251 received the following flight modifications:

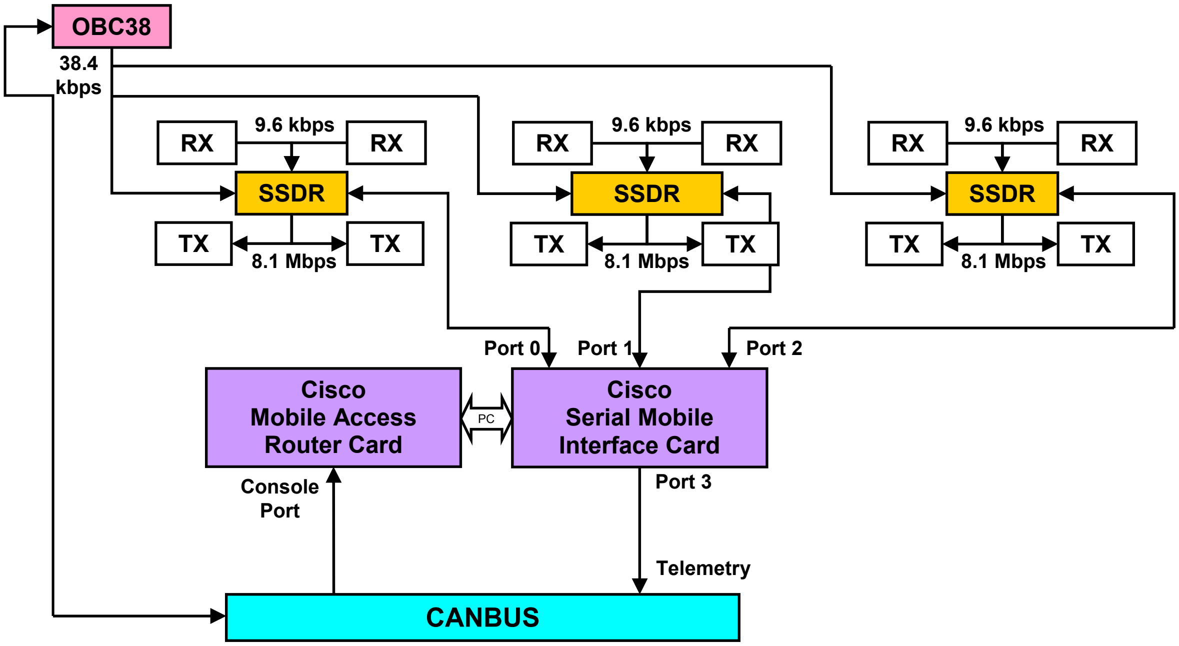
a. All terrestrial connectors were removed and replaced with point-to-point wiring.
b. All liquid filled components were removed and replaced with equivalent, non-liquid filled parts.
c. High heat rejection devices were provided a thermal path for heat rejection to the primary structure.

The CISCO 3251 was NOT modified to provide additional radiation tolerance. It successfully survived full, flight-level qualification testing (vibration, thermal vacuum, etc…) on the first attempt. Currently, the CISCO 3251 appears to be operating as expected on orbit (voltage and current readings are nominal). Data flow tests have not yet been conducted (they are awaiting software modifications to the solid state data recorder).

The DMC platform is very IP “friendly”, but is not itself truly IP compliant (it utilizes a CANBUS automotive bus and proprietary Solid State Data Recorders [SSDRs] to manage the flow of data). The satellite does use the following on board:

- Use of IP protocols on all flight computers
  - HDLC framing
  - Frame Relay encapsulation
- Housekeeping
  - Use of standard (proprietary) SSTL protocols for TM/TC
    - Modified for use over IP
    - Translation layer written to allow maximum reuse of existing SSTL flight software (AX.25 / IP)
  - TCP connection for telecommand
  - UDP employed for file transfer
- Payload
  - Use of Selective Negative ACK file transfer protocol over UDP
    - Either MDP or CFDP

The on board satellite network (Figure H) consists of two redundant receivers (RX 0 and 1) and transmitters (TX 0 and 1) which communicate with three redundant solid state data recorders (SSDR 1100, 0, and 1). The SSDRs are also connected to the redundant flight computers (one, OBC 386 is shown). The flight computers are also connected to the CANBUS, which is, in turn, independently connected to the receivers and transmitters and used as a primary command path. The four serial ports of the CISCO 3251 are connected as shown (Ports 0, 1, and 2 are each connected to one of the SSDRs, Port 3 is connected to the CANBUS and will be used to download telemetry data from the experiment). The router console port is also connected to the CANBUS. It will likely be used as a path for router configuration changes. It should be noted that there is not a direct path from the router to the flight computers and that all satellite commanding will need to be accomplished through ground station interactions. In the current design, the SSDRs act like routable devices (i.e. a “flat” network), effectively “hiding” the space-based router from the ground-based network. To overcome that deficiency (inherent to the generic SSTL satellite) Surrey engineers intend to perform a SSDR software modification which causes one SSDR (SSDR 1100 most likely) to act like a “piece of wire” or pass through device. Once this software modification has been successfully accomplished, the path for router operations will be from the appropriate ground station, through one of the two receivers, through SSDR 1100, to the router via Port 1. Once router access has been achieved, typical network activities (like moving a file from SSDR 0 to SSDR 1 [or to the ground]) can be performed. It may also be possible to sequentially uplink, store, and build large router image files in the SSDR for eventual use with router reconfiguration.



DMC On Board Network Configuration
Figure H

To ensure that the software modification works correctly, Cisco has also procured a flight like SSDR, CANBUS, and flight modified CISCO 3251 router from SSTL. This device (essentially a flatsat or satellite on a bench) will be housed at GRC and used to verify all operations prior to use on the actual flight element. Additionally, the VMOC will be connected to the device to verify interfaces and satellite commanding, prior to execution.

All of SSTL's spacecraft are controlled from their fully automated control room, located at their primary site in Surrey, England (Figure I). The control room monitors fifteen satellites and actively controls nine using three independent antennas. Software is used extensively to monitor and interact with the space vehicles (human intervention is typically not required for routine operations). Anomalies are also detected through software and notifications are made to the appropriate flight personnel via pager or mobile phone. Satellite recovery operations can be conducted locally or through a generic Internet connection.

SSTL Satellite Operations Centre
Surrey, England
Figure I

Ground Infrastructure and Operations

The demo is broken into several scenarios, and the associated Concept of Operations has been designed to incrementally test the Virtual Mission Operations Center capabilities. The remote users will have access to the VMOC using appropriate desktop or laptop computers with VPN client and biometric sensors installed. User access to the spacecraft command, control, and data, is made using browser software and a tunnel to the remotely located VMOCs. The spacecraft is RF linked to a ground-station that tunnels through the Internet to the same VMOCs. The primary VMOC is physically located in a safe haven with the shadow VMOCs running in disparate locations. Intrusion detection hardware and software will be monitoring all traffic coming in and out of both VMOCs. The VMOCs will be operated in a pilot / co-pilot mode with one functioning as the prime controller and the other shadowing the operations so a rapid handoff can be made in the event the primary VMOC failed. The primary VMOC will be located in the Center for Research Support (CERES) at Schriever AFB, with the co-pilot VMOC located on NASA's Glenn Research Center in Cleveland Ohio. In addition, there will be a test bed VMOC located at a General Dynamics site in Los Angeles. The test bed VMOC will allow offline test and evaluation associated with system changes expected from lessons learned. Each VMOC will determine the appropriate level of access each user should have and enable them to only see/control their authorized elements. All system access requests and responses will be archived to meet non-repudiation requirements.

A typical user session would occur as follows:

1. As a user logs in, DoD Public Key Infrastructure (PKI) Common Access Cards (CAC), password, and biometrics provide user authentication. Once validated, the VMOC establishes a secure session with the user. During the session, the VMOC watches for command appropriateness and command / user prioritization, ensuring the right person, at the right time, is issuing the appropriate command.

2. The user is presented with a web page that allows him/her to navigate to authorized systems / sensors. The user's options can include live command, control, and information; scheduling future command, control and information, or requesting products derived from stored data. Command requests require the user to again authenticate via a biometric device to ensure the current operator is the original user that logged into the session and authorized to perform the requested operation.

3. For field users making simple data requests, the VMOC Mission Integrator module first attempts to match the user's data and latency requirements from existing databases. If the information is available, the user is routed directly to the data, or the data is passed to the user. If the information is not already available in an existing database and the request requires sensor / system actions, the Mission Integrator continues with additional checks ensuring that no mission rules, contention control, or user priorities are violated. In doing this, the Mission Integrator interfaces with both the Condition Monitor and Scheduling modules. The Condition Monitor contains mission rules, current values, and system conditions; while the Scheduler contains pre-allocated user access time and mission/platform operations schedules. If for any reason a user request cannot be fulfilled, the Mission Integrator informs the user of the denial and the reason.

4. Where connectivity is not constant and bandwidth is asymmetric, the Intelligent Multiplexer module orchestrates command and telemetry requirements based on mission rules, time, priorities and bandwidth availability. The intent is to optimize network utilization and maximize benefit to the user.

The VMOC utilizes a layered defense in depth security philosophy and it is continuously monitored by a Secure Network Operations Center, where network perimeter defenses are kept updated and operational and action is taken in the event of cyber attack. Running on an intranet and introducing multi-level security can add additional capabilities (including data and command compartmentalization) to this architecture.

Risk Mitigation

As with any new technology, especially those never flown before in space, a certain element of mission risk is present. To help mitigate that risk a number of strategies have been implemented as a part of this project:

1. Extensive ground tests have been conducted on the miniature router to ensure that it is fully compatible with existing terrestrial systems and capable of performing the actions necessary in flight.

2. Cisco has purchased additional equipment from SSTL for further ground tests. This equipment is flight qualified and emulates the hardware in space exactly. This equipment (a modified miniature router, solid state data recorder, and CANBUS) will be used to demonstrate tests and system configurations prior to use on the flight element.

3. The VMOC, which is platform independent, will be developed in parallel with the router system on the ground. Although it needs a router in space for the final integrated tests, it can be tested with other platforms (including the emulated flight element) to ensure that it is operating as expected. In the unlikely event that the flight article aboard the spacecraft is incapable of operations, a substitute platform will be utilized to demonstrate the integrated capability.

Follow-on Activities

The expected lifetime of the router experiment in space is five years. Following a successful demonstration of the router and VMOC capabilities, additional testing is expected. Possible follow-on activities include:

1. A demonstration of linked, cooperative systems. The satellite could be used to queue other IP-based systems to perform integrated tasks. These other systems may be located in aircraft, ships, on the ground, or aboard other satellites. Discussions are currently under way with the UAV community concerning the likelihood of future collaborative testing.

2. A demonstration of autonomous, ground-based satellite instrument calibration. Researchers will use the VMOC to queue up a satellite pass at a specific location, at a specific time. Data collected during the pass will then be compared to data collected in-situ at the same time and location.

Conclusions

A joint network centric demonstration is currently underway, with participation from NASA GRC, the Air Force and Army Space Battle Labs, NASA GSFC, Cisco, Western DataCom, Surrey Satellite Technologies Limited, and General Dynamics. This demonstration will highlight the flight of COTS network device (a miniature router) aboard an experimental micro-satellite that is controlled remotely using an Internet Protocol-based satellite command and control application that provides secure, virtual mission operations. The new architecture, showcased through this demonstration, is intended to meet the security, survivability, and rapid re-configuration requirements typically found in a complex research or battlefield environment. The results of this demonstration are intended to be used by those designing and fielding future integrated land, sea, air, and space core network elements.

References

1. Asrar, Ghassem Ph.D., “*A Message from the Associate Administrator for Earth Science*,” Earth Science Enterprise Strategic Plan. October 1st, 2003.

2. Earth Science Enterprise Strategic Plan. October 1st, 2003. pp1-2.
3. Earth Science Enterprise Strategic Plan. October 1st, 2003. p 3.
4. Earth Science Enterprise Strategic Plan. October 1st, 2003. pp10-11.
5. Earth Science Enterprise Strategic Plan. October 1st, 2003. p 41.
6. ESTO web page: http://esto.nasa.gov/info_technologies_aist1.html.
7. NSA “*Information Assurance Technology Framework*” CD. September 2002. p 2-4.
8. NSA “*Information Assurance Technology Framework*” CD. September 2002. p 1-10.

Contact Information

Name	Organization	Phone #	Email Address
Phil Paulsen	NASA GRC	216-433-6507	phillip.e.paulsen@nasa.gov
Will Ivancic	NASA GRC	216-433-3494	william.d.ivancic@nasa.gov
Terry Bell	NASA GRC	216-433-3725	terry.l.bell@grc.nasa.gov
Dave Stewart	NASA GRC	216-433-9644	david.h.stewart@grc.nasa.gov
Don Van Drei	NASA GRC	216-433-9089	donald.e.vandrei@nasa.gov
Dan Shell	Cisco	440-331-5663	dshell@lint.cisco.com
Lloyd Wood	Cisco	44-20-8824-4236	lwood@mrwint.cisco.com
Phil Ardire	Western DataCom	440-835-1510	phil@western-data.com
Eric Miller	General Dynamics	805-606-8626	eric.miller@gd-ais.com
Jon Walke	General Dynamics	805-606-8626	jon.walke@gd-ais.com
Steve Groves	Space and Missile Defense Command Battle Lab	719-544-4166	steven.groves@arspace.army.mil
Brett Conner	Air Force Space Battle Lab	719-567-9512	brett.conner@schriever.af.mil
Larry Dikeman	Air Force Space Battle Lab	719-567-0442	larry.dikeman@schriever.af.mil